DELIBERATIVE STUDY OF VANET SIMULATION TOOLS WITH EMPHASIS ON PRIVACY AND SECURITY

Amit B. Parmar
Asst.Prof., Department of Information Technology, AITS, Rajkot, India

Paras P. Kalariya
Asst.Prof., Department of Information Technology, AITS, Rajkot, India

Rahul N. Vaza
Asst.Prof., Department of Computer Engineering, AITS, Rajkot, India

Pinali N. Katariya
PG Student, Department of Information Technology, AITS, Rajkot, India

Anju K. Kakkad
Asst.Prof., Department of Computer Engineering, AITS, Rajkot, India

Abstract—Vehicular networks are likely to become the most relevant form of mobile ad hoc networks. The deployment of vehicular communication (VC) systems is strongly dependent on their security and privacy features. The primary objectives of the architecture include the management of identities and cryptographic keys, the security of communications, and the integration of privacy enhancing technologies. The security of Vehicular Ad Hoc Networks (VANET) has mostly directed the attention of today research efforts, while comprehensive solutions to protect the network from adversary and attacks still need to be improved, trying to reach a satisfactory level, for the driver and manufacturer to achieve safety of life and infotainment. Vehicular communication system facilitates communication devices for exchange of information among vehicles and vehicles and Road Side Units (RSUs). The era of vehicular adhoc networks is now gaining attention and momentum. In this paper, we address the security of these networks. We provide a detailed threat analysis and devise an appropriate security architecture. The need for a robust VANET networks is strongly dependent on their security and privacy features, which will discussed in this paper. This paper presents a comparative study of various publicly available VANET simulation tools.

Keywords—MANETs, VANET, ad-hoc networks, RSUs, Wireless, Security Inter-Vehicular Communications, Authentication, Simulation

I. INTRODUCTION

Until recently, road vehicles were the realm of mechanical engineers. But with the plummeting costs of electronic components and the permanent willingness of the manufacturers to increase road safety and to differentiate themselves from their competitors, vehicles are becoming “computers on wheels”, or rather “computer networks on wheels”. For example, a modern car typically contains several tens of interconnected processors; it usually has a central computer as well as an Event Data Recorder, reminiscent of the “blackboxes” used in avionics. Optionally, it also has a GPS receiver, a navigation system, and one or several radars. Manufacturers are about to make a quantum step in terms of vehicular IT, by letting vehicles communicate with each other and with roadside infrastructure; in this way, vehicle swill dramatically increase their awareness of their environment, thereby increasing safety and optimizing traffic.

Considering the tremendous benefits expected from vehicular communications and the huge number of vehicles (hundreds of millions worldwide), it is clear that vehicular communications are likely to become the most relevant realization of mobile ad hoc networks. The appropriate integration of on-board computers and positioning devices, such as GPS receivers along with communication capabilities, open tremendous business opportunities, but also raise formidable research challenges.

One of these challenges is security; very little attention has been devoted so far to the security of vehicular networks. Yet, security is crucial. For example, it is essential to make sure that life-critical information cannot be inserted or modified by an attacker; likewise, the system should be able to help establish the liability of drivers; but at the same time, it should protect as far as possible the privacy of the drivers and passengers.

These concerns may look similar to those encountered in other communication networks, but they are not. Indeed, the size of the network, the speed of the vehicles, the relevance of their geographic position, the very sporadic connectivity between them, and the unavoidably slow deployment make the problem very novel and challenging. The purpose of this paper is to bring a first response to this challenge.
After the deployment of various vehicular technologies, such as toll collection or active road signs, vehicular communication (VC) system shave emerged. They comprise network nodes, that is, vehicles and road-side infrastructure units (RSUs) equipped with onboard sensory, processing, and wireless communication modules. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication can enable arange of applications to enhance transportation safety and efficiency, as well as infotainment. For example, they can send warnings about environmental hazards (e.g., ice on the pavement), traffic and road conditions (e.g., emergency braking, congestion, or construction sites), and local (e.g., tourist) information.

II. VANETS SECURITY SERVICES DESIGN REQUIREMENT

The very high speed of real-time constraint is the unique characteristic of VANETs. All the security services should meet strict time constraints; otherwise, the service will become void. Different prospects warrant distinct protocols; thereby, they emerge different types of protocol specifications. The security requirements listed below are not necessarily relevant to all aspects of network specification and all applications. The requirements are quite standalone. They can be viewed as building blocks towards more complex specifications. The security services of VANETs generally contain the following requirements:

A. Authentication:

The authentication service is concerned with assuring that the communication is authentic in its entities. Vehicle should react to events only with disseminating messages generated by legitimate senders. Therefore we need to authenticate the senders of these messages.

B. Integrity:

The integrity service deals with the consistency of a stream of messages. It assures that messages are received as sent, without modification, insertion, reordering, or replays.

C. Non-repudiation:

This service prevents either sender or receiver denying a transmitted message. This service may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident.

D. Confidentiality:

This service protects the privacy of the communication content. It guarantees the privacy of drivers against unauthorized observers.

E. Availability:

A kind of attacks can result in the loss or reduction in the availability. Even a robust communication channel can still suffer some attacks (such as deny-of-service) which can bring down the network. Therefore, availability should be also supported by alternative means.

III. SYSTEM ASSUMPTIONS

A. Network model

The communicating nodes in VANETs are either vehicles or base stations. Vehicles can be private (belonging to individuals or private companies) or public (i.e., public transportation means, e.g., buses, and public services such as police cars). Base stations can belong to the government or private service providers. We assume a communication channel supported by an IEEE 802.11-like technology. Given that the majority of the network nodes will consist. There are two kinds of communicating entities in VANETs. The first node is vehicle which is the majority of the network nodes. The second node is the roadside base station. The communication channel is supported by an IEEE 802.11-p technology. Vehicular communication proof vehicles, the network dynamics will be characterized by quasi-permanent mobility, high speeds, and (in most cases) very short connection times between neighbors (e.g., in the case of crossing vehicles). For example, on highways vehicle speeds are usually higher than 80km/h (with relative speed will require nodes to communicate directly (if node is the range of transmission) or across multiple wireless links(hops). Nodes will act both as end points and routers. VANET will enable both vehicle-to-vehicle and vehicle-to-roadside. The former can be often the only way to realize safety and driving assistance applications.
Figure 3.1: vehicles and road-side base stations that exchange primarily safety messages.

B. Application categories

There are many applications in vehicular communication, most of which are proposed by the vehicle manufacturers. These applications are divided into two major categories:

1. **Safety-related applications** such as collision avoidance, cooperative driving, and traffic optimization. The common characteristic of this category is the relevance to life-critical situations where the existence or lack of a service may affect life-endangering accidents. Hence the security of this category is mandatory, since the proper operation of any of these applications should be guaranteed regardless of the presence of security threats.

2. **Other applications**, including payment services (e.g., toll collection), location-based services (e.g., finding the closest fuel station), infotainment (e.g., Internet access). Obviously, security is also required in this application category, especially in the case of payment services. But in this paper we address the security aspects of safety-related applications because they are the most specific to the automotive domain and because they raise the most challenging problems.

C. Safety messages

As explained in the previous section, we consider only public safety applications. In this context, we can classify the safety messages into three classes, based on their properties related to privacy and real-time constraints, as shown in Table I. Traffic information messages are used to disseminate traffic conditions in a given region and thus affect public safety only indirectly (by preventing potential accidents due to congestion); hence they are not time-critical. General safety-related messages are used by public safety applications such as cooperative driving and collision avoidance and hence should satisfy stringent constraints such as an upper bound on the delivery delay. Liability-related messages are distinguished from the previous class because they are exchanged in liability-related situations such as accidents. Therefore, the liability of the message originator should be determined by revealing his identity to the law enforcement authorities. This classification of messages will be useful later in describing the attacks on VANETs. Messages are distinct from the previous class. They are exchanged in liability-related situations such as accidents. For this kind of liability-related information, the message originator should be adjudicated by disclosing user’s identity to the law enforcement authorities.

### Table I. Message Classes and Properties

<table>
<thead>
<tr>
<th>Class/Property</th>
<th>Legitimacy</th>
<th>Privacy protection against other individuals</th>
<th>Privacy protection against the police</th>
<th>Real-time constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic information</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>General safety messages</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Liability-related messages</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

IV. ATTACKS AND THREATS

In this paper we are concentrating on attacks perpetrated against the message itself rather than the vehicle, as physical security is not in the scope of this paper.

Denial of Service attack. This attack happens when the attacker takes control of a vehicle’s resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving. It also increases the danger to the driver, if it has to depend on the application’s information. For instance, if a malicious wants to create a massive pile up on the highway, it can make an accident and use the DoS attack to prevent the warning from reaching to the approaching vehicles [2], [8], [9], and [10]. See figure 2. The authors in [11], proposed a solution by switching between different channels or even communication technologies (e.g., DSRC, UTRA-TDD, or even Bluetooth for very short ranges), if they are available, when one of them (typically DSRC) is brought down.
Cheating with positioning information: Attackers in this case are also I m .R.A, and use this attack to alter their perceived position, speed, direction, etc. in order to escape liability, notably in the case of an accident. In the worst case, colluding attackers can clone each other, but this would require retrieving the security material and having full trust between the attackers.

ID disclosure of other vehicles in order to track their location. This is the Big Brother scenario, where a global observer can monitor trajectories of targeted vehicles and use this data for a range of purposes (e.g., the way some car rental companies track their own cars). To monitor, the global observer can leverage on the roadside infrastructure or the vehicles around its target (e.g., by using a virus that infects neighbors of the target and collects the required data). The attacker is passive. We assume that the attacker does not make use of cameras, physical pursuit, or onboard tracking devices to uncover the identity of his target; otherwise, the tracking problem becomes simpler but also more expensive and tied to few specific targets, and it can be done anyhow based on existing license plates. In addition, we assume that physical-layer attacks (e.g., using radio finger printing are solved by appropriate physical layer techniques such as radio transmitters that randomize finger prints.

Masquerade: The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives.

V. SECURITY REQUIREMENT

A. Tamper-proof device

The use of secret information such as private keys incurs the need for a tamper-proof device in each vehicle. In addition to storing the secret information, this device will be also responsible for signing outgoing messages. To reduce the risk of its compromise by attackers, the device should have its own battery, which can be recharged from the vehicle, and clock, which can be securely resynchronized, when passing by a trusted roadside base station. The access to this device should be restricted to authorized people. For example, cryptographic keys can be renewed at the periodic technical checkup of the vehicle. Several commercial products have these features.

B. Digital signatures

As emphasized in Section A, message legitimacy is mandatory to protect VANETs from outsiders, as well as misbehaving insiders. But since safety messages will not contain any sensitive, confidentiality is not required. As a result, the exchange of safety messages in a VANET needs authentication but not encryption. Symmetric authentication mechanisms usually induce less overhead per message (not counting the handshake needed to establish a shared key) than their asymmetric counterparts. But digital signatures are a better choice in the VANET setting, because safety messages are typically standalone, as mentioned in Section 3.1.3 and should be sent to receivers as fast as possible. In fact, a preliminary handshake is not acceptable and actually creates more overhead. In addition, given the huge amount of network members and the sporadic connectivity to authentication servers, a PKI (Public Key Infrastructure) is the most suitable way for implementing authentication.

C. Tamper-proof device

The use of secret information such as private keys incurs the need for a tamper-proof device in each vehicle. In addition to storing the secret information, this device will be also responsible for signing outgoing messages. To reduce the risk of its compromise by attackers, the device should have its own battery, which can be recharged from the vehicle, and clock, which can be securely resynchronized, when passing by a trusted roadside base station. The access to this device should be restricted to authorized people. For example, cryptographic keys can be renewed at the periodic technical checkup of the vehicle. Several commercial products have these features.

D. DoS resilience

DoS attacks are the nightmare of security experts, since they are mounted with no rational purpose and hence are very difficult to prevent, especially in a wireless medium. To mitigate these attacks, we propose switching between different channels or even
communication technologies (e.g., DSRC, UTRA-TDD, or even Bluetooth for very short ranges), if they are available, when one of them (typically DSRC) is brought down. In the worst-case scenario (i.e., when no means of communication between vehicles exist), the VANET enhanced features (e.g., collision avoidance) should automatically turn off to avoid problems until the network is reestablished. In fact, this is likely to be the default option in the early days of VANETs, when only a few vehicles will have the necessary technology.

VI. SIMULATION TOOL FOR VANET

We have classified existing VANET simulation software into three different categories. They are (a) Vehicular mobility generator (b) Network simulator (c) VANET simulators.

VANET mobility generators are used to generate realistic movement traces of the vehicles motion to increasing level of realism in VANET simulation. These traces subsequently imported into a network simulator as an input in order to study the performance of the protocol application. Network simulators perform detailed packet-level simulation of source, destinations, reception, route, background load, links, data traffic transmission and channels. Finally, VANET simulators provide both network simulation and traffic flow simulation. In the next few sections, we will discuss vehicular mobility generators, network simulators and VANET simulators in greater depth with their characteristics, functions.

VANET mobility generators are used to generate realistic movement traces of the vehicles motion to increasing level of realism in VANET simulation. These traces subsequently imported into a network simulator as an input in order to study the performance of the protocol application. In this section we present the different vehicular mobility generators and a comparison of them.

Simulation of Urban Mobility (SUMO) is an open source, highly portable microscopic road traffic simulation package that deals very large number of nodes in vehicular ad hoc network. It can be used on most of the operating system. Because of high portability and its GNU General public license SUMO has become more popular and most widely used in vehicular ad hoc networks. Citymob is a highly portable, open source, GUI based mobility model generator generally used in Vehicular adhoc Networks (VANETs). Citymob implements three different Mobility models: (a) Simple Model(SM), (b) Downtown model (DM) and (c) Manhattan Model (MM). The main advantages of Citymob is that it is portable, open source, ease of setup and easy to use. But its biggest limitations is that it generated traces does not support NS-2, GloMoSim, QualNet, SWANS. And also real and user defined maps is not available here. The increasing popularity and attention in VANETs has prompted researchers to develop realistic and accurate simulation tools. In this paper, we make a comparative survey of several publicly available mobility generators, network simulators, and VANET simulators. The mobility generators studied include SUMO, VanetMobiSim, MOVE, Citymob and FreeSim. MOVE, VanetMobiSimand SUMO all have traffic model supports and good software features However, only VanetMobiSim provides excellent trace supports. FreeSim and Citymob both provide good software characteristics.

VII. CONCLUSION

Inter-Vehicular Communications (IVC) are a key feature of the future intelligent transportation systems. A crucial enabling component of IVC is its security services. In this paper, we reviewed the secure infrastructure and discussed the security issues and attacks on VANETs. Then we discussed also the major threats. Using the analysis obtained in the related work, we have come to a certainty result that existing network security solutions are not sound enough and what kind of possible treats are there on them.

Finally, we have discussed the available simulators and its characteristic and performance in real time system. In general we had discussed all security concerned to VANATs.

References


